ZKTeco FR1200 User Manual

Version: 1.0.1

Date: Dec. 2011

Introduction:

This document introduces the user operations of the ZKTeco FR1200. For device installation, please refer to the Installation Guide.

Table of Contents

1. Using Instruction ..... - 1 -

1.1 Finger Placement ..... - 1 -
1.2 Instruction for Card Using ..... - 1 -
1.3 Precautions ..... - 1 -

2. Device Introduction ..... - 3 -

3. Device Operations ..... - 5 -

4 Appendix ..... - 8 -

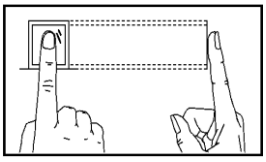
4.1 List of Parameters ..... - 8 -
4.2 Statement on Human Rights and Privacy ..... - 9 -
4.3 Environment-Friendly Use Description ..... - 10 -

1. Instruction for Use

1.1 Finger Placement

Enroll fingerprint by pressing the index finger, middle finger or ring finger (thumb and little finger are clumsy).

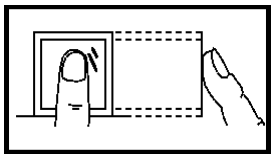
1. Proper press:



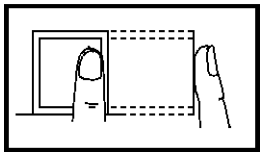
Center the finger on the sensor window and press.

2. Improper press:

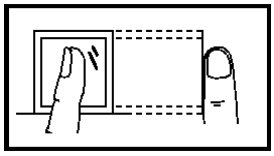
Upright



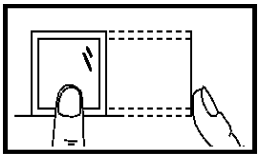
Off Center



Slanted



Off Center



Please adopt the correct way to place the finger to avoid improper operation leading to identification performance degradation.

1.2 Instruction for Card Use

Integrated with a non-contact RF card reader module, this reader supports the ID cards and Mifare cards (Optional and only used as ID cards). By offering multiple verification modes such as FP, card, FP plus card, FP or card verification, this reader can accommodate diversified user needs.

Swipe your card across the sensor area following the light and beep prompts and remove your card after the reader has sensed it. For the card sensor area information, please refer to section 2 Device Introduction in this manual.

1.3 Precautions

Protect the reader from exposure to direct sunlight or strong beams of sunlight. Strong sunlight greatly affects the fingerprint collection and leads to fingerprint verification failure.

It is recommended to use the reader under a temperature of 0–50°C so as to achieve optimal performance. In the event of exposure of the

reader to the outdoors for long periods of time, it is recommended to adopt sunshade and heat dissipation facilities because excessively high or low temperatures may slow down the reader operation and result in high false rejection rate (FRR) and false acceptance rate (FAR).

When installing the reader, please connect the power cable after all the other wiring. If the reader does not operate properly, be sure to shut down the power supply before performing necessary inspection. Be aware that any live-line working may cause damage to the reader and that damage is beyond the scope of our normal warranty.

For matters that are not covered in this document, please refer to related materials including the Installation Guide and FP Reader Software User Manual.

2. Device Introduction

FR1200, a fingerprint reader with RS485 communication interface works with biometric access controllers and fingerprint standalone access control. It offers the ability to capture and transfer fingerprint samples to access control panel inside to match. With its IP65 rated rugged structure, this reader operation is simple and flexible. The light and beep prompts will guide you through all the operations without screen display or keyboard. Featuring a compact and simple design, this reader is a new concept of inBIO fingerprint reader.

Product Appearance:

Front view:

- **LED indicator:** The LED indicator is used to display reader operation results and exceptional statuses which are defined as follows:

  Operation Succeeds: The green indicator is solid on for one second, at the same time the speaker plays one long beep.

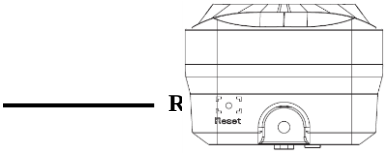
  Operation Failed: The red indicator is solid on for one second, at the same time the speaker plays two short beeps.

  Verification State: The green LED blinks once every two seconds. The beeper makes no sound.

- **Card Sensor Area:** Refers to the area in the red dashed-line as shown in the figure above.

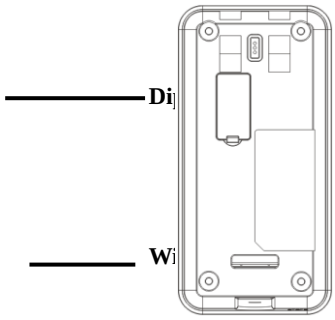
- **Fingerprint Sensor:** Used to enroll and match fingerprints.

Bottom view:



- **Reset Button:** Used to restart the reader.

Back view:



Dip Switch: 1-4 switches are used to set the RS485 communication address (device ID). Number 5 switch is idle. And the number 6 switch is used to set the terminal resistance state.

Wiring Terminal: For connecting terminals.

3. Device Operations

After the reader is powered on, the reader cannot identify a fingerprint or card. In other words, the reader cannot receive data or send data without an access control panel connection.

Only when the reader is connected with the access control panel can the reader prompt if the card or fingerprint is enrolled or not, and verify the user according to the returning result of background access control panel.

User Verification Operations:

1. When the reader is connected with the access control panel, it is in verification state, the green LED blink once every two seconds to prompt verification.

2. Start user verification. The reader supports four verification modes: only fingerprint, only card, fingerprint plus card, and fingerprint or card verification. The process includes pressing the fingerprint first or swiping the card first, the operations are as the follows:

Pressing the Fingerprint First:

(1) Properly press your finger on the fingerprint sensor. The device beeps once, and then the LED goes off and switches to the background verification.

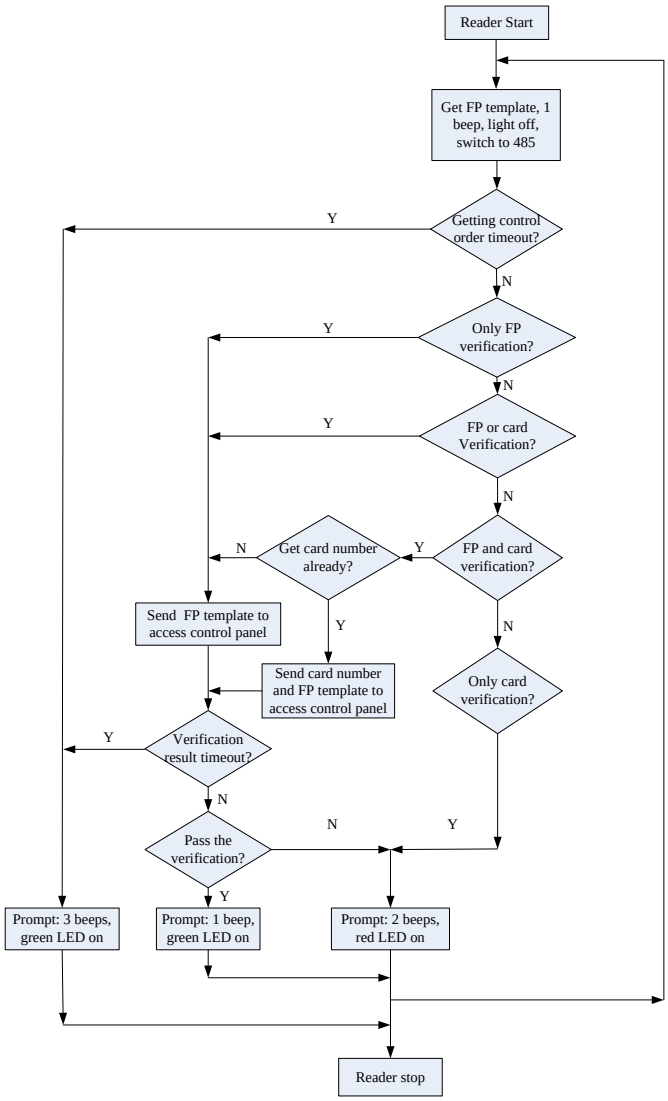
(2) The access control panel determines whether the control order times out. If it does time out, the device beeps 3 sounds and the red LED goes solid on. Otherwise, it will get the system verification modes setting.

Only fingerprint/card or fingerprint verification: Send the fingerprint template to the access control panel, and wait for the result. If it times out, it will beep 3 times and the red LED goes solid on. If the reader gets the verification result in the setting time, it will beep 2 times and the red LED goes solid on for verification failed and beep 1 time with a green LED solid on for verification succeed.

Card plus fingerprint verification: Determine if there is card data. Swipe the card near the card reader and send a fingerprint template and card data to the access control panel and wait for the result. If it times out, it will beep 3 times and the red LED goes solid on. If the reader gets the verification result within the setting time, it will beep 2 times and the red LED goes solid on for verification failed, or beeps 1 time and the green LED goes solid on for verification succeed.

Only card verification: No sending of data to the access control panel. The device beeps 2 times and the red LED goes solid on.

The verification operations are as follows:



Swipe Card First:

(1) Swipe your card on the card reader. The device beeps once, and then the LED goes off and switches to the background verification.

(2) The access control panel determines whether the control order times out. If it times out, the device beeps 3 times and the red LED goes solid on. Otherwise, it gets the system verification modes setting.

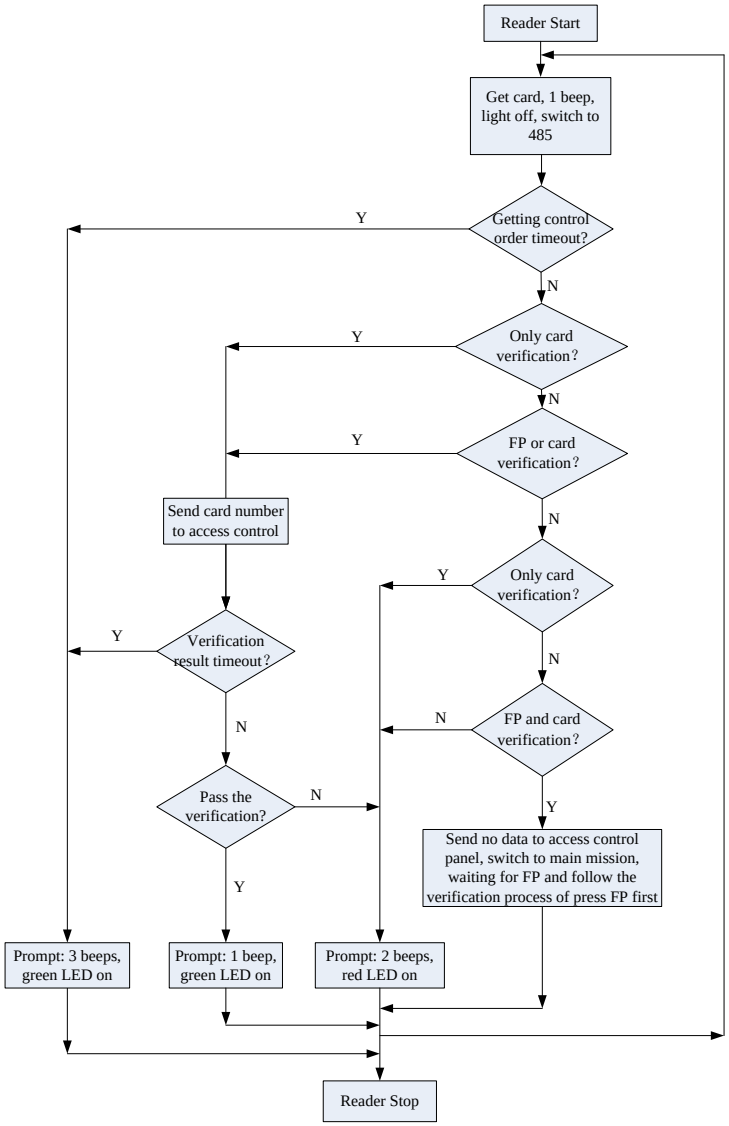
Only Card/Card or Fingerprint Verification: Send the card data to the access control panel and wait for the result. If it times out, it beeps 3 times and the red LED goes solid on. If the reader gets the verification result within the time setting, it beeps 2 times and the red LED goes solid on for verification failed or beeps 1 time and the green LED goes solid on for verification succeed.

Card Plus Fingerprint Verification: Determine if there is fingerprint data. If it times out, it beeps 3 times and the red LED goes solid on. Otherwise, it follows the card plus fingerprint verification with the fingerprint press first.

Only Fingerprint Verification: No sending of the data to access control panel, the device beeps 2 times and the red LED goes solid on.

Note: For the verification mode setting, please refer to the FP reader software user manual or relevant software user manual.

The verification operations are as follows:



4 Appendix

4.1 List of Parameters

The following table lists the basic functional parameters of the reader.

Item	Note
Power Supply	DC12V/3A
External Function	EXT 485 for access control panel connection
Verification mode.	ID (Mifare) card, fingerprint
Communications	RS485
Speaker	Beep prompt
LED	Bi-color indication (red/green)

4.2 Statement on Human Rights and Privacy

Dear Customers:

Thank you for choosing the multi-biometric products designed and manufactured by us. As a world-renowned provider of biometric technologies and services, we pay much attention to the compliance with the laws related to human rights and privacy in every country while constantly performing research and development.

We hereby make the following statements:

1. All of our fingerprint recognition readers for civil use only collect the characteristic points of fingerprints instead of the fingerprint images, and therefore no privacy issues are involved.

2. The characteristic points of fingerprints collected by our products cannot be used to restore the original fingerprint images, and therefore no privacy issues are involved.

3. We, as the equipment provider, shall not be held legally accountable, directly or indirectly, for any consequences arising due to the use of our products.

4. For any dispute involving human rights or privacy when using our products, please contact your employer directly.

Our fingerprint products or development tools for police use support the collection of the original fingerprint images. As for whether such a type of fingerprint collection constitutes an infringement of your privacy, please contact the government or the final equipment provider. We, as the original equipment manufacturer, shall not be held legally accountable for any infringement arising thereof.

Note: The law of the People's Republic of China has the following regulations regarding personal freedom:

1. Unlawful arrest, detention or search of citizens of the People's Republic of China is prohibited; infringement of individual privacy is prohibited.

2. The personal dignity of citizens of the People's Republic of China is inviolable.

3. The home of citizens of the People's Republic of China is inviolable.

4. The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law.

At last we stress once again that biometrics, as an advanced recognition technology, will be applied in a lot of sectors including e-commerce, banking, insurance and legal affairs. Every year people around the globe suffer from great loss due to the insecurity of passwords. The fingerprint recognition actually provides adequate protection for your identity under a high security environment.

4.3 Environment-Friendly Use Description

The Environment Friendly Use Period (EFUP) marked on this product refers to the safety period of time in which the product is used under the conditions specified in the product instructions without leakage of noxious and harmful substances.

The EFUP of this product does not cover the consumable parts that need to be replaced on a regular basis such as batteries and so on. The EFUP of batteries is 5 years.

Names and Concentration of Toxic and Hazardous Substances or Elements

Parts Name	Toxic and Hazardous Substances or Elements					
	Pb	Hg	Cd	Cr6+	PBB	PBDE
Chip resistor	×	○	○	○	○	○
Chip capacitor	×	○	○	○	○	○
Chip inductor	×	○	○	○	○	○
Chip diode	×	○	○	○	○	○
ESD components	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

×: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part is above the limit requirement in SJ/T11363-2006.

Note: 80% of the parts in this product are manufactured with non-hazardous environment-friendly materials. The hazardous substances or elements contained cannot be replaced with environment-friendly materials at present due to technical or economical constraints.